

UNITED STATES DISTRICT COURT
FOR DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF:
(1) a White iPhone, with Assigned Evidence
Property # 22-5418-PR, Currently Located at
Nashua Police Department, Nashua, NH; (2) a
Black smart phone, with Assigned Evidence
Property # 22-5417-PR, Currently Located at
Nashua Police Department, Nashua, NH; and
(3) a Black Samsung smart phone with IMEI
354327823391825, Currently Located at
Nashua Police Department, Nashua, NH

Case No. 23-mj-4-01-AJ

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Adam Terrizzi, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—namely three phones:

- a. a white iPhone in a clear and black trimmed case seized from Chuck Genao the day of his arrest in Nashua, assigned Evidence Property Number 22-5418-PR, and located in the evidence locker at the Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062 (“Device A”);
- b. a black smart phone in a black case seized from Darrell Regular the day of his arrest in Nashua, assigned Evidence Property Number 22-5417-PR, and located at Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062 (“Device B”); and

- c. a black Samsung smartphone with IMEI 354327823391825 discovered on January 6, 2023 in a pocket behind the driver seat in the red minivan pursuant to a search warrant executed by Nashua Police Department and currently located at 28 Officer James Roche Dr, Nashua, NH, 03062 (“Device C”);

all of which are electronic mobile devices currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachments B-1, B-2, and B-3.

2. I am a Special Agent (SA) with the United States Secret Service and have been so employed since May 24, 2021. I am currently assigned to the Manchester, New Hampshire Resident Office. In preparation for my employment with the United States Secret Service I completed the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center in Glynco, Georgia. Additionally, I completed the Special Agent Training Course (SATC) at the United States Secret Service James J. Rowley Training Center in Laurel, Maryland. While attending SATC I received a five-day training titled “Basic Investigation of Computer and Electronic Crimes Program” (BICEP). In addition to these training programs, I have completed numerous in-service training courses related to constitutional law. Prior to my employment with the United States Secret Service, I was a full-time certified Police Officer in Manchester, New Hampshire for over five years. My present duties include the investigation of federal offenses, including, but not limited to, those involving financial fraud and its related activities.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The first property to be searched, described here and in Attachment A-1, is a white iPhone in a clear and black trimmed case seized from Chuck Genao the day of his arrest in Nashua, assigned Evidence Property Number 22-5418-PR, and located in the evidence locker at the Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062, hereinafter “Device A.”

5. The applied-for warrant would authorize the forensic examination of Device A for the purpose of identifying electronically stored data particularly described in Attachment B-1.

6. The second property to be searched, described here and in Attachment A-2, is a black smart phone in a black case seized from Darrell Regular the day of his arrest in Nashua, assigned Evidence Property Number 22-5417-PR, and located at Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062, hereinafter “Device B.”

7. The applied-for warrant would authorize the forensic examination of Device B for the purpose of identifying electronically stored data particularly described in Attachment B-2.

8. The third property to be searched, described here and in Attachment A-3, is a black Samsung smartphone with IMEI 354327823391825 discovered on January 6, 2023 in a pocket behind the driver seat in the red minivan pursuant to a search warrant executed by Nashua Police Department and currently located at 28 Officer James Roche Dr, Nashua, NH, 03062, hereinafter “Device C.”

9. The applied-for warrant would authorize the forensic examination of Device C for the purpose of identifying electronically stored data particularly described in Attachment B-3.

PROBABLE CAUSE

10. On the evening of December 6, 2022, Chuck Genao, born in 1988, and Darrel Regular, born in 1959, were together when they were arrested in Nashua, New Hampshire by officers of the Nashua Police Department. Genao was charged with Identity Fraud, Posing as Another, and Theft by Deception. Regular was charged with Identity Fraud, Posing as Another, and two misdemeanor counts of Theft by Deception.

11. The conduct underlying the arrests of Genao and Regular in Nashua, New Hampshire involved the fraudulent use of other people's identity information to open and use credit accounts at stores associated with the TJX Companies.¹

12. A white iPhone in a clear and black trimmed case was seized from Genao during the booking procedure. It was assigned Evidence property control number 22-5418-PR and is in the evidence locker at the Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062.

13. A black smartphone phone in a black case was seized from Regular during the booking procedure. It was assigned Evidence property control number 22-5417-PR and is in the evidence locker at the Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062.

Background: Credit Card Fraud Scheme at TJX Stores and Involvement of Genao and Regular

¹ The TJX Companies, Inc. ("TJX"), are a Multinational off-price apparel and home fashions retail group based in Framingham, MA. They operate approximately 4,700 stores under five brands: TJ Maxx, Marshalls, HomeGoods, Sierra Trading Post, and HomeSense. Credit cards opened at these stores, i.e., TJX Rewards Credit Cards, are opened in conjunction with Synchrony Financial ("Synchrony"), a financial services company which provides the financial backing to the cards.

14. On December 6, 2022, Nashua Police were alerted to the presence of Genao and Regular by Jeffrey Saddig, a Retail Fraud Investigator employed by TJX. For several months, Saddig has been looking into a pattern of organized retail theft and identity theft involving multiple individuals, including two individuals believed to be Genao and Regular.

15. Since mid-2022, Saddig also has provided information to Special Agent (SA) Matthew Flynn of the U.S. Secret Service and Task Force Officer (TFO) Matthew Hogan of the Connecticut State Police who are investigating a multi-state scheme involving offenses including wire fraud, in violation of 18 U.S.C. § 1343, aggravated identity theft, in violation 18 U.S.C. § 1028A, access device fraud, in violation of 18 U.S.C. § 1029, and conspiracy, in violation of 18 U.S.C. § 371 as well as 18 U.S.C. § 1349, and other offenses.

16. In the course of their investigation, SA Flynn and TFO Hogan have obtained various video and still images from the Closed Circuit Television (“CCTV”) systems at TJX stores in in several states, including Connecticut, Massachusetts, Florida, Texas, and Illinois. The images, which span the timeframe of March 2022 through December 2022, were captured when TJX credit cards were fraudulently applied for at TJX store registers and used soon after to make purchases of store gift cards or merchandise. SA Flynn and TFO Hogan observed that two individuals, who appear to be Genao and Regular, are seen repeatedly on the video images engaged in the fraudulent activity. At times, two other individuals appear to be with them, as well.

17. SA Flynn and TFO Hogan also have collected documentary and other evidence and have learned that, frequently, (1) the names and identity information used to apply for the TJX credit cards belong to individuals with addresses in the general geographical region of the TJX store, (2) the victims did not authorize the credit account applications, and (3) the victims

were unaware of their information being used in connection with these credit accounts. SA Flynn and TFO Hogan also learned that the merchandise purchased using the fraudulent credit cards would later be returned at other TJX store locations. Similarly, Store Value Cards (“SVCs”), more commonly known as gift cards, would be exchanged at other TJX locations. These returns and exchanges often resulted in the proceeds being transferred to other bank cards.

Discovery of Genao and Regular in New Hampshire on December 6, 2022

18. On December 6, 2022, TJX Investigator Saddig discovered Genao and Regular were in Nashua, NH based on information received from another TJX Retail Fraud Investigator and information he viewed via TJX’s CCTV systems. More specifically, Saddig received information from TJX Investigator Kaitlyn Peabody indicating that a male individual at a Sierra Trading Post in Bedford, NH, had opened a new TJX Rewards Credit Card account and immediately attempted to purchase SVCs. When Saddig reviewed a still image sent out by Peabody (taken from TJX’s CCTV video system) which showed the male who opened the possibly fraudulent account, Saddig recognized the male in the photo to be consistent with Darrel Regular.

19. Previously, Saddig had seen evidence that Genao and Regular often visited several TJX stores in the same region within a short timeframe. Accordingly, the TJX investigator(s) began reviewing high-dollar transactions at other TJX stores in New Hampshire.

HomeGoods #128 in Bedford, NH on December 6, 2022

20. Information from HomeGoods Store #128, at 9 Kilton Road, Bedford, NH, and CCTV video images revealed two high dollar transactions that day: a \$1,200.00 purchase of SVCs at 1:23 pm by one male individual, and another \$1,200.00 purchase of SVCs at 1:25 pm by

a different male individual. Saddig recognized that one of the males appeared consistent with Regular and the other appeared consistent with Genao.

21. Still photos of both males were provided to SA Flynn and TFO Hogan. SA Flynn and TFO Hogan had previously reviewed government identification and photographs for Genao and Regular. SA Flynn and TFO Hogan concluded that the male individuals in the Bedford HomeGoods Store #128 photos were consistent with Genao and Regular. In terms of clothing, Genao was wearing a red hooded sweatshirt and blue hat/cap, jeans, and white sneakers. Regular was wearing black pants, black shoes, dark blue shirt, dark blue jacket, gray hat/cap, and a face mask.

22. Further investigation revealed that the males in the still photos from the Bedford HomeGoods Store #128, i.e., Genao and Regular, utilized the identities and social security numbers of C.B. (born in 1955), and K.B. (born in 1967), respectively, to make the \$1,200.00 purchases of SVCs.

TJX Stores in Nashua, NH on December 6, 2022

23. Saddig also reviewed CCTV footage from the surrounding TJX stores and believed one of the suspects may have been at HomeGoods #114, 12 Northwest Boulevard, Nashua, NH.

24. Via live CCTV footage, Saddig observed that an individual who appeared to be Regular was at Marshalls Store #441, 28 Northwest Boulevard, Nashua, NH; this information was ultimately conveyed to the Nashua Police Department along with a request that the area be checked for Genao and Regular.

25. Saddig was able to observe that Genao and Regular were utilizing a maroon colored minivan with partial Connecticut registration "B70456." Additional information from

Saddig indicated that the suspects had changed location to TJ Maxx #356, located at 590 Amherst Street, Nashua, NH. Genao and Regular appeared to be wearing clothing similar to that they wore in the Bedford HomeGoods Store #128.

26. On December 6, 2022, at 5:56 pm Officer Wade Hanson of the Nashua Police Department located a red-colored Chrysler Pacifica minivan, with Connecticut registration BE70456, exiting the parking lot of TJ Maxx #356 onto Amherst Street. Officer Hanson followed the vehicle as it pulled into a BP Gas Station on Amherst Street and made contact with the vehicle occupants when the vehicle stopped.

27. Officer Hanson subsequently identified the three occupants of the vehicle as Genao, Regular, and Samuel Horne. Regular was identified by his NY driver's license. Genao initially provided a false name to the officer, but his description matched the one provided via radio including wearing a red top and blue hat, and a subsequent record check on Genao revealed that he had two warrants, one from Maryland which was extraditable and the other from Florida.²

28. SA Flynn, TFO Hogan, and Saddig communicated with Detective Roach of the Nashua Police Department on December 6, 2022, regarding the investigation into fraudulent activity at TJX stores in multiple states. Given the possibility of fraudulent activity at other TJX stores in New Hampshire that day, Saddig further reviewed the TJX CCTV video system, including video from Marshalls Store #441 in Nashua and TJ Maxx Store #356 in Nashua. Based on transaction information and CCTV surveillance video, Saddig learned that Genao and Regular had visited these stores and apparently had opened TJX Credit Cards using identity information belonging to other individuals at TJ Maxx Store #356.

2

29. SA Flynn and TFO Hogan also viewed the still images of both suspects from inside HomeGoods Store #114, Marshalls Store #441 and TJ Maxx Store #356, and concluded that the individuals in the still images were consistent with Genao and Regular.

30. Officer Anderson of the Nashua Police Department learned from staff at TJ Maxx Store #356 that Regular had opened up a TJX Rewards Credit Card in the name of L.V. (born 1961) of Nashua, NH, using L.V.'s social security number, at 5:42 pm on December 6, 2022. Regular had also purchased \$400.00 of TJX Company SVCs using a temporary shopping pass from the approved L.V. credit card. In addition, Genao had opened a TJX Rewards Credit Card at TJ Maxx Store #356, in the name of G.L., (born 1968) of Nashua, NH, using G.L.'s social security number at 5:47 pm. Genao then purchased \$400.00 of TJX Company SVC's using a temporary shopping pass from the approved G.L. credit card.

31. At Marshalls #441 in Nashua, NH, Det. Roach of the Nashua Police Department spoke with Assistant Store Manager Alexandria Monaco. Monaco provided a credit card customer verification slip from Marshalls concerning the TJX credit card application in the name of C.C. (born 1954) of Nashua, NH. This slip was for a credit card Regular had applied for and subsequently used to purchase \$391.68 of store merchandise. Det. Roach also received a receipt for \$900.00 for prepaid SVCs purchased by Genao under the name G.C. (born 1966) of Nashua, NH. These purchase amounts were confirmed by a representative of Synchrony Financial.

32. At HomeGoods #114 in Nashua, NH, Det. Roach spoke with employee Julia Carney who provided a customer verification slip concerning the TJX credit card application in the name of G.C. This slip was for a credit card applied for by Regular and later utilized by Genao at Marshalls #441 for the purchase of \$900 in SVCs referenced above.

33. On December 8, 2022, Synchrony provided SA Flynn and TFO Hogan with information regarding the names possibly used on fraudulent TJX Credit Card applications at locations in New Hampshire. This information included 13 identities of individuals listed as living in Southern New Hampshire or Massachusetts and included the 4 identities used by Genoa and Regular at TJX locations in Nashua, NH, i.e., G.L., G.C., C.C., and L.V. These four individuals were contacted by Det. Roach of the Nashua Police Department in relation to the accounts opened in the Nashua TJX locations. Each person confirmed to Roach that they had not opened any TJX Rewards credit cards or given permission for anyone to use their information to do so.

Use of Mobile Devices During Fraudulent Activity in New Hampshire

34. SA Flynn and TFO Hogan also learned that T.S., an employee working at Marshalls on December 6, 2022, had tended to the customer who applied for the TJX credit account in the name of C.C.. (The customer was identified by law enforcement as Darrel Regular.) T.S. recalled that the customer received several calls while at the store and appeared to be communicating with someone outside the store to convey that he would be out soon.

35. Based on information from Saddig and a representative of Synchrony Financial, SA Flynn and TFO Hogan learned that Regular was captured on CCTV during the \$391.68 purchase made with the newly-opened account in the name of C.C. During the transaction, at approximately 5:28 pm on December 6, 2022, Regular can be seen using his mobile device.

36. Similarly, SA Flynn and TFO Hogan learned that while at TJ Maxx store #356 in Nashua, NH, Chuck Genao is viewed on CCTV video while opening a new TJX MasterCard account using an ID in the name of G.L. During the application process and while entering

information into the Customer PIN Pad, Genao can be seen at approximately 5:46 pm on December 6, 2022 referring to his mobile device.

37. The maroon minivan Genao and Regular were riding in is registered to EAN Holdings, LLC (EAN) (Operating as Enterprise, Alamo, and National car rental companies). Regular reported that he was the renter of the vehicle. SA Flynn subsequently learned that the vehicle had been rented at JFK Airport in New York by Darrel Regular for the dates November 16, 2022 through December 7, 2022. EAN further reported that Regular utilized the email address darrelregular543@gmail.com and the phone number 210-932-6861 to reserve the rental vehicle. This is the same telephone number that appears on the Evidence Property tag #22-5417-PR for the black smart phone seized from Regular's during his arrest (Device B).

38. On December 6, 2022, Nashua Police Officers observed, in plain view within the rental vehicle, a Marshalls shopping bag with unknown contents, crumpled receipts scattered throughout the passenger compartment, multiple TJX Company SVCs in the storage pouch behind the driver's seat, and multiple TJX Credit Card application pamphlets.

39. On January 6, 2023, Nashua Police Officers discovered during the execution of a state search warrant for the maroon minivan, a black Samsung smartphone with IMEI 354327823391825 which was discovered in a pocket behind the driver seat in by members of the Nashua Police Department and is currently located at 28 Officer James Roche Dr, Nashua, NH, 0306, i.e., (Device C);

40. SA Flynn and TFO Hogan observed via bodycam that Genao was seated in the minivan behind the driver's seat at the time it was stopped by Nashua Police and thus would have been the person in the vehicle with most ready access to that seat pocket when the car was

stopped by police. Again, they were stopped on a day when that vehicle and Genao were at several TJX stores involved in the credit card fraud and identity theft activities under investigation.

41. On December 6, 2022, during a search incident to arrest during the booking process at the Nashua Police Department, Genao was found in possession of a Visa debit card bearing the name of C.G. and a HomeSense SVC (in addition to Device A). During a search incident to arrest, Regular was found in possession of bank cards, TD Bank account ID cards with different account numbers, a HomeGoods Temporary Shopping Pass in the name of C.C., and the bottom portion of TJX Credit Card applications in the names of J.G. and M.P. (in addition to Device B).

Historical Information Concerning Use of Mobile Devices by Genoa and Regular

42. SA Flynn and TFO Hogan have learned over the course of this investigation that Genoa and Regular have been seen on CCTV footage with their cell phones in the vicinity of the registers and, at times, referencing a cell phone when entering information into Customer PIN pads while filling out TJX Credit Card applications. Examples include:

a. On March 28, 2022 at HomeGoods #844 in Southbury, CT, a male later identified by investigators as Genao is seen presenting a TJX Credit Application to a cashier. Genao, with a cell phone in his left hand, begins to refer to his cell phone as he is entering information into the Customer PIN Pad during the application process. Genao is then seen signing the Customer Verification Slip utilizing the identity of A.Q. (born 1968) of Danbury, CT. Genao was issued a Temporary Shopping Pass ending in 9009. The loss amount of this transaction was \$1,200.00.

b. On April 10, 2022 at HomeSense #001 in Framingham, MA, a male later identified by investigators as Genao is seen on CCTV footage presenting a completed TJX Credit Application to a cashier. Genao, with a cell phone in his left hand, begins to enter information into the Customer PIN Pad during the application process. Genao is then seen signing the Customer Verification Slip utilizing the identity of J.M. (born 1968) of Framingham, MA. Genao was issued a Temporary Shopping Pass ending in 3318. The loss amount of this transaction was \$1,197.99.

c. On August 21, 2022 at Marshalls #1042 in Oldsmar, FL, a male later identified by investigators as Genao is seen on CCTV footage presenting information to open a new TJX Credit Card to a cashier. Genao is then seen referring to his cell phone, located in his left hand, as he is entering information into the Customer PIN Pad during the application process. Genao is then seen signing the Customer Verification Slip utilizing the identity of D.C. (born 1965) of Clearwater, FL. Genao was issued a Temporary Shopping Pass ending in 7562. The loss amount of this transaction was \$899.59.

d. On October 14, 2022 at TJ Maxx #481 in Bloomingdale, IL, a male later identified by investigators as Regular is seen on CCTV footage standing in the register line. Regular has a cell phone in his left hand, pulls down his face mask with his right hand, and holds the cell phone up to his mouth. Regular then applied for a TJX Credit Card using the identity of G.T. of Tinley Park, IL. Regular was issued a Temporary Shopping Pass ending in 0699 and used it to buy two \$200.00 SVCs. The loss amount of this transaction was \$400.00.

Genao and Regular Have Traveled to Various States During the Scheme

43. SA Flynn and TFO Hogan have reviewed not only CCTV surveillance images, but also various documentary records collected over the course of the investigation. They learned that Genao and Regular have been seen between March 2022 and December 2022 in numerous TJX locations in Connecticut, Massachusetts, Florida, Texas, New Hampshire, Illinois, and elsewhere. The total fraud loss from this scheme, based on identifiable transactions linked to Genao and Regular, is approximately \$125,000, with 200 different identities used.

44. SA Flynn and TFO Hogan have reviewed records which show Genao and Regular traveled interstate via commercial airline and utilized rental cars during the period of the scheme. At times, others have traveled with them as well. Records also show that Genao and Regular listed their mobile device numbers and email addresses to purchase airline tickets and rent cars during the course of the scheme.

45. Based on my training and experience, I know that reservation information for airlines and rental cars are commonly sent to customers via email and text, and that such information is often stored in cell phones and used during the period of travel. I also know that receipts associated with these activities are often sent via text and email. Further, I know that cell phones commonly contain location information in various forms, including for example, searches for addresses and directions to locations like various TJX stores in a particular region. Moreover, through my training and experience, I am aware that individuals involved in identity theft and who attempt to use the identity data of multiple individuals in a short timeframe can require reminders as to certain numbers, e.g., social security numbers, zip codes, street addresses, and I know that having a cell phone in hand can provide access to the information quickly and easily.

46. In sum, based on the information learned in this investigation, the information indicates that Genao and Regular have been involved in a credit card fraud and identity theft scheme that has spanned March through December 2022, and targeted TJX stores and identity theft victims in several states. Further, evidence collected indicates that Genoa and Regular have had access to and, and times, used their cell phones during the fraudulent activity. Moreover, their phone numbers are associated with travel-related services which are often accessed via cellphone during trips, i.e., airline reservations and rental car reservations. Further, two of the cell phones were seized from Genao and Regular on December 6, 2022 when they were arrested for fraudulent conduct consistent with the scheme currently under investigation. Accordingly, it is more probable than not that information related to the offenses and scheme under investigation, are contained within Devices A, B, and C.

47. The Devices are currently in the lawful possession of the Nashua Police Department. As described above, Devices A and B came into their possession when they were seized incident to arrest during the booking of Genao and Regular on December 6, 2022, and Device C was discovered when law enforcement executed a search of the maroon minivan in which Genoa and Regular were traveling on the day of their arrest. Therefore, while the Nashua Police Department might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

48. The Devices are currently in storage at the evidence locker at the Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062. SA Flynn and TFO Hogan have received information indicating that the Devices have been stored in a manner in which their contents are preserved.

TECHNICAL TERMS

49. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellr telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable

storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When

a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. **Pager:** A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

50. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available online I know that Devices A,B, and C have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience,

examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

51. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

52. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices A, B, and C, were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices A, B, and C, because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

53. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent

with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

54. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

55. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachments A-1, A-2, and A-3 to seek the items described in Attachments B-1, B-2, and B-3.

Respectfully submitted,

/s/ Adam Terrizzi

ADAM TERRIZZI

Special Agent

UNITED STATES SECRET SERVICE

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Jan 6, 2023**

Time: **5:15 PM, Jan 6, 2023**





HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-2

The property to be searched is a black smart phone in a black case seized from Darrell Regular the day of his arrest in Nashua, assigned Evidence Property Number 22-5417-PR, and located at Nashua Police Department, 28 Officer James Roche Dr, Nashua, NH, 03062, hereinafter the “Device B.”

This warrant authorizes the forensic examination of the Device B for the purpose of identifying the electronically stored information described in Attachment B-2.

ATTACHMENT B-2

1. All records on the Device B described in Attachment A-2 that relate to violations of wire fraud, in violation of 18 U.S.C. § 1343, aggravated identity theft, in violation 18 U.S.C. § 1028A, access device fraud, in violation of 18 U.S.C. § 1029, conspiracy, in violation of 18 U.S.C. § 371 as well as 18 U.S.C. § 1349, and related offenses, and involve Chuck Genao, Darrell Regular, or other individuals, since March 1, 2022, including:

- a) Incoming and outgoing calls; incoming, outgoing, and draft text, picture messages, video messages, social media messages; and incoming and outgoing e-mails, detailing telephone data communications, including cell site location information; any estimated, approximate or known GPS/latitude and longitude location of these cellular devices locations for the period of March 1, 2022 to December 6, 2022, range to tower (RTT), TrueCall, TDOA or Timing Advanced Information and per call measurement (PCM) data, cell site information to include all known cell towers associated with outgoing and incoming calls, cell site locations, any estimated, approximate or known longitude and latitude, any information recovered from cell phone towers in reference to direction and distance from the tower a device may be located (timing and triangulation information) as well as similar data that has been deleted from the telephone but may still be extracted from the device;
- b) Still photographs, video clips, and audio clips from the telephone's internal memory, as well as similar data that has been deleted from the telephone but may still be extracted from the device;
- c) Any passwords or unlock codes necessary to access the internal data within the device;

- d) BIOS settings, registry settings (including MRU or “Most Recently Used” keys), “P-List” files, which are often used to store a user’s settings and can assist in the forensic examination of the user’s Apple devices, directories, file names, and properties, user information, application software, operating system(s);
- e) Records and information in whatever form and by whatever means they may have been created or stored in the devices, including electrical, electronic, or magnetic, on any internally installed drives, floppy disks or memory data cards;
- f) Graphic images, still photographs, slides, video clips, visual mediums, and any record, file, or data of their origins, or any other visual depictions of such graphic interchange format equipment that may be, or are evidence in violation of Title 18, United States Code, Sections 1028A, 1029, 1343, 1349, and 371;
- g) Internet browsing history with cell site location information, user ID’s and passwords for Internet web sites and third-party applications (Facebook, Instagram, WhatsApp, TextNow, etc), web sites visited, search engine terms used by persons utilizing the devices;
- h) Text messages, SMS, MMS, instant messaging, and third-party applications (such as KIK, Twitter, Snapchat, Facebook messenger, Whisper, WhatsApp, TextNow, and like applications)
- i) Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, from March 1, 2022 to 12/6/2022 calendar entries, notes, alerts, invites, and invitees. This information can assist in establishing the plans and/or location of the owner / user of the account and connections to other suspects;

- j) Contacts & Groups - All contacts including name, all contact phone numbers, emails, social network links, and images, as well as groups & group listings and group ID's associated with target account. This information can assist in establishing identity the owner / user of the account and connections to other suspects;
- k) Maps - All information to include recent search history, location history and location service data between the dates of March 1, 2022 to 12/06/2022. Such data shall include GPS coordinates, dates and times of all location recordings. Such information would assist in identifying preplanned routes or searches for directions to the location of other accomplices, co-conspirators, or victim;
- l) Associated Applications - All applications downloaded, installed, and/or purchased related to the device. Such information could provide additional information to linked applications that contains data responsive to this search warrant request;
- m) Wallet/Checkout/Bank Information - All information contained in the associated digital storage device including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers, as well as all bank records, checks, credit card bills, account information, and other financial records showing ownership of accounts. Such evidence can help to verify the identity of the cellphone owner and related accounts, as well as show illicit transactions;
- n) Application, Cloud Storage & Social Media Account Information - User name, user identification number, primary email address, secondary email addresses, connected applications and sites, including account sign in locations, browser information, platform information, and Internet protocol (IP) addresses, as well as other application data, including but not limited to Facebook Messenger, Whisper, Snapchat, WhatsApp,

TextNow, Bandwidth or other messaging, communication or other social media applications allowing communication or exchange of data between people, and/or cloud or other remote storage accounts upon which communications, images or other files or data can be archived or stored. This information can establish identity of the owner, other potential applications and communications platforms potentially used by the suspect to communicate with other accomplices, co-conspirators or victim, and other sources of data that would be responsive to this search warrant request;

- o) Data Backup Files – Access to any data backup folders identified during the examination of this cellphone that may contain evidence responsive to this search warrant request, including but not limited to encrypted data folders or files, and /or cloud or remote storage folders or accounts in which such data can be archived or stored.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.